ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

Secure Transformation of Data in Encrypted Image Using Reversible Data hiding Technique

S.Poongodi M.E., (Ph.D), Assistant Professor (Sr), K.S.R college of Engineering, Tiruchengode
Dr.B.Kalavathi, Professor and Head, K.S.R Institute of Engineering and Technology, Tiruchengode
M.Shanmugapriya, PG/VLSI Design, K.S.R college of Engineering, Tiruchengode

Abstract: ***Reversible data hiding is a technique that is used to hide data inside an image for high security. The data is hidden in such a way that the exact or original data is not visible. The hidden data can be retrieved as when required. The proposed scheme of reversible data hiding technique is achieved through colour image instead of gray scale image to improving the capacity of hidden data. Initially for more privacy protection content owner encrypt the original image using encryption key. Then, compress the LSB bits to create a sparse space for accommodating hidden data using data hiding key. By using both the keys the receiver can extract hidden data and recover the original image without any error. If the receiver has only data hiding key or only encryption key, such that the receiver can get only hidden data or only decrypted image.***

Index Terms: **Image Encryption, Reversible data hiding, Image and data Recovery.**

I. INTRODUCTION

Digital communication has become an essential part of infrastructure. Now a day, a lot of applications are internet-based and it is important that communication made be a secret. As a result, the security of information passed over an open channel has become a fundamental issue and therefore, the confidentiality and data integrity are required to protect against unauthorized access. This has resulted in an unstable growth in the field of information hiding. Encryption is the most effective way to achieve data security. The process of Encryption hides the contents of a message in a way that the original information is recovered only through a decryption process. The purpose of Encryption is to prevent unauthorized parties from viewing or modifying the data. Image encryption is an effective approach to protect images or videos by transforming them into completely different formats. Several data encryption algorithms like Data Encryption Standard (DES) and Advanced Encryption standard (AES) are being employed for protecting digital information. In this paper a simple encryption method is used by bit XOR operation [1].

The encrypted image can be compressed by using several techniques. In Lossy compression of an encrypted image flexible compression ratio is done[3]. The original image is encrypted by pseudorandom permutation, and then compressed by discarding the excessively rough and fine information of coefficients in the transform domain. When having the compressed data and the permutation way, an iterative updating procedure is used to retrieve the values of coefficients by exploiting spatial correlation in natural image, leading to a reconstruction of original principal content.

The compression ratio and the quality of reconstructed image vary with different values of compression parameters. The higher compression ratio and the smoother original image is the better quality of the reconstructed image. The reversible data hiding scheme in encrypted image [5] with a low computation complexity is proposed, which consists of image encryption, data embedding and data extraction/ image-recovery phases. The data of original image are entirely encrypted by a stream cipher. Although a data-hider does not know the original content, data hider can embed additional data into the encrypted image by modifying a part of encrypted data. Through an encrypted image containing embedded data, a receiver may firstly decrypt it using the encryption key, and the decrypted version is similar to the original image. According to the data-hiding key, with the aid of spatial correlation in natural image, the embedded data can be correctly extracted while the original image can be perfectly recovered.

In Separable reversible data hiding in encrypted image[1] . The content owner encrypts the original uncompressed image using an encryption key. Although a data-hider does not know the original content, can compress the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. Through an encrypted image containing additional data, the receiver may extract the additional data using only the data-hiding key, or obtain an image similar to the original one using

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

only the encryption key. When the receiver has both of the keys, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image if the amount of additional data is not too large.

II. REVERSIBLE DATAHIDING

Reversible data hiding is a technique to embed additional message into some distortion-unacceptable cover media, such as military or medical images, with a reversible manner so that the original cover content can be perfectly restored.

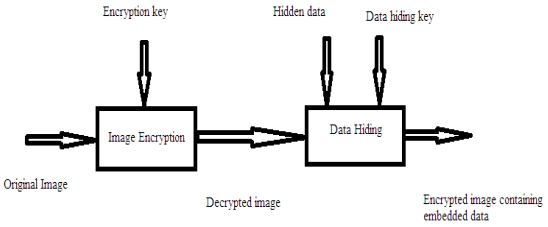

Fig.1.Data hiding in Encrypted image

A number of reversible data hiding methods have been proposed in recent years. In difference expansion method [5], differences between two adjacent pixels are doubled to generate a new least significant bit (LSB) plane for accommodating additional data. A data hider can also perform reversible data hiding using a histogram shift mechanism [8], which utilizes the zero and peak points of the histogram of an image and slightly modifies the pixel gray values to embed data into the image. Another kind of method makes use of redundancy in a cover by performing lossless compression to create a spare space for data embedding [3]. Furthermore, various skills have been introduced into the typical reversible data hiding approaches to improve the performance.

III. PROPOSED SCHEME

The proposed scheme of reversible data hiding technique is achieved through colour image instead of gray scale image to improving the capacity of hidden data. Initially for more privacy protection content owner encrypt the original image using encryption key. Then, compress the LSB bits to create a sparse space for accommodating hidden data using data hiding key. By using both the keys the receiver can extract hidden data and recover the original image without any error. If the receiver has only data hiding key or only encryption key, such that the receiver can get only hidden data or only decrypted image. Figure 1 explains, the content owner encrypt the original colour image using an encryption key and embedding the hidden data in encrypted image using data hiding key which is done in sender side.

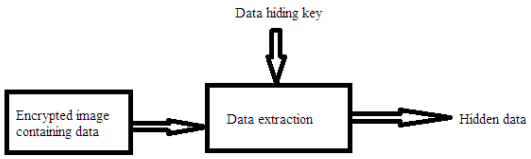

Fig.2.1 Option 1-Data extraction

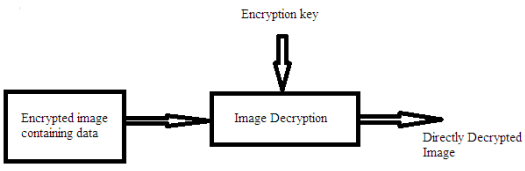

Fig. 2.2 Option 2-Image decryption

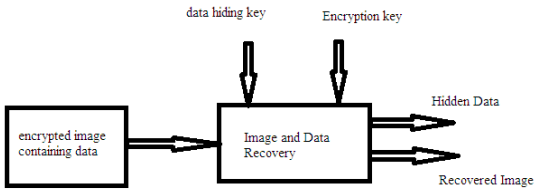

Fig. 2.3 Option 3-Data and image recovery

Fig.2. Three options in receiver side

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

A. Image Encryption

Assuming original colour image size is N1*N2 and each pixel of red, green, blue value falling into [0,255] is represented by 8 bits. Denote each bits of a pixel represented as bj,k,0 ,bj,k,1 , . . .bj,k,7 where 1≤j≤N1 and 1≤k≤N2, and the rgb value as qj,k. Denote the other number of pixels as N(N=N1XN2).

$B_{j,k,a} = [q_{j,k,a}/2^a]\bmod 2,\ a=0,1,.....7$ (1)

and

$q_{j,k} = \sum_{a=0}^{7}[bj,k,a]2^a$ (2)

$B_{j,k,a} = b_{j,k,a} + r_{j,k,a}$ (3)

In encryption phase original bits and pseudo-random bits are calculated by exclusive-or. Where $r_{j,k,a}$ are determined by an encryption key using a standard stream cipher.

B.Data Embedding

In the data embedding, some parameters D,H,R are embedded into a small number of encrypted pixels, and the other encrypted pixels of LSB are compressed to creating a sparse space for accommodating the additional data. The detailed procedure is as follows. After encrypting the original colour image content owner pseudo-randomly selects Nt encrypted pixels according to a data hiding key that will be used to carry the parameters (D,H,R) for data hiding. Here, Nt is a small positive integer. The other N-Nt encrypted pixels are pseudo-randomly permuted and divided into a number of groups using data hiding key, each group contains no of pixels which is denoted as H. Collect the D least significant bits of the H pixels in each group, which is denoted by B(g,1),B(g,2),.....B(g,D,H) where g is a group index within [1,$(N-N_t)/H$] and D is a positive integer less than 5. Here, S is a small positive integer

The content owner generates a M matrix which has two parts by (4).

$M = [I_{D.H-R}\ \ F]$ (4)

Where $I_{D.H-R}$ is an identity matrix $I_{D.H-R}$ = (D.H-R) X (D.H-R)and F = (D.H-R)XR which is derived from the data-hiding key. Then, The parameters D,H, and R embedded into the LSB of N_t. For example if N_t=16 the values of D,H and R are represented as 2, 12 and 2 bits respectively, and N_t LSB encrypted pixels replaced by 16 bits. In following, a total bits made up of N_t and $(N-N_t).R/H-N_t$ additional bits will be embedded into the pixel groups. For each group, calculate

$$\begin{matrix} B'(g.1) \\ \dots \\ B'(g.D.H-R) \end{matrix} = F \begin{matrix} B'(g.1) \\ \dots \\ B'(g.D.H) \end{matrix} \quad (5)$$

Which is determined by modulo-2. For data accommodation compress the bits of B(g,1),B(g,2),.....B(g,D.H) as (D.H-R) bits. In each group, the original LSB of selected encrypted pixels and the additional data to be embedded as [B'(g,D.H-R+1),B'(g,D.H-R+2).....B'(g.D.H)]. Then, replace the new [B'(g,1),B'(g,2)....B'(g,D.H)], with B(g,1),B(g,2),.....B(g,D.H) and put into their original positions by reversible manner. At the same time, the most significant bits (MSB) of encrypted pixels are kept unchanged. Since bits are embedded into each pixel-group, the total $(N-N_t).R/H$ bits can be accommodated in all groups. Figure 3 shows the original input image and figure 4 shows the result of encrypted image containing embedded data.

C. Data Extraction and Image Recover

In this phase, there are three options at the receiver side; These three options are shown in figure 2.

a) If the receiver has only data hiding key, receiver can extract the data and does not know about the original content.

b) If the receiver has only encryption key, receiver can decrypt the image and does not know about the hidden data.

c) If the receiver has both encryption and data hiding key, receiver can extract the data and also recover the original content.

(a)In first option, with an encrypted image containing embedded data, receiver may first obtain the values of the parameters D,H and R from the LSB of the N_t selected encrypted pixels. Then, the receiver permutes and divides the other $(N-N_t)$ pixels into $(N-N_t)/R$ groups and extracts the R embedded bits from the D LSB-planes of each group. When having the total $(N-N_t)R/H$ extracted bits, the receiver can divide them into N_t original LSB of selected encrypted pixels and $(N-N_t)R/H-N_t$ additional bits.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

Note that because of the pseudo-random pixel selection and permutation, any attacker without the data-hiding key cannot obtain the parameter values and the pixel-groups, therefore cannot extract the embedded data. Furthermore, if the receiver having the data-hiding key can successfully extract the embedded data, receiver cannot get any information about the original image content.

Fig.3.orginal image

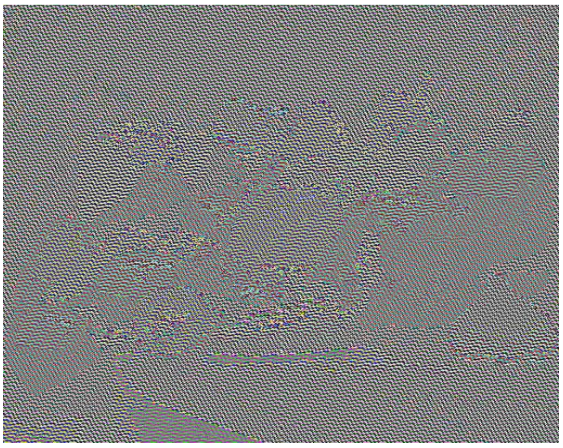

Fig.4.Encrypted image containing data

(b) In second option, if the receiver has the encryption key but does not know the data-hiding key. Clearly, receiver cannot obtain the parameter values therefore cannot extract the embedded data. However, the original image content can be roughly recovered using encryption key. Denoting the bits of pixels in the encrypted image containing embedded data as $B'_{j,k,0}$, $B'_{j,k,1.....}$ $B'_{j,k,7}$ the receiver can decrypt the data

$$b'_{j,k,a}=B'_{j,k,a}+r_{i,k,a} \qquad (6)$$

The rgb values of decrypted pixels are

$$P'_{j,k}=\sum_{a=0}^{7}[bj,k,a]2^{a} \qquad (7)$$

Figure 5 shows the result of directly decrypted image using decryption key.

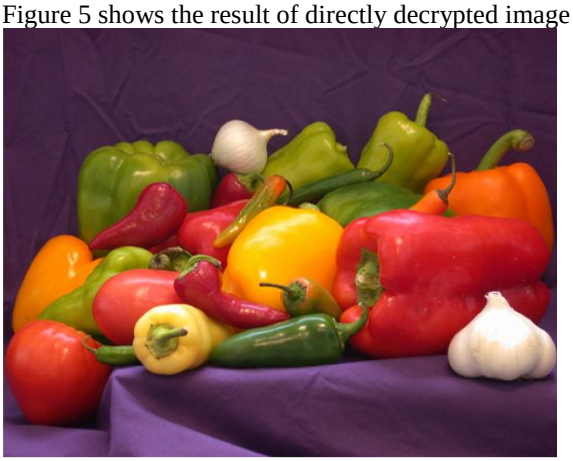

Fig.5.Directly decrypted image

Fig.6.Decrypted image

The decrypted MSB must be same as the original MSB. Since the data-embedding operation does not alter any MSB of encrypted image. So, the content of decrypted image is similar to that of original image.

If B(g.D.H-R+1)=B(g.D.H-R+2)=.....=B(g.D.H-R)=0 there is

$$B'(g.x)=B(g.x). \quad x=1,2,.....D.H-R. \qquad (8)$$

The probability of this case is $1/2^{R}$ and the original bits in D LSB-planes can be decrypted correctly. Since R is significantly less than D.H.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

The distortion energy per each decrypted pixel is

$D_E=2^{-2D}\sum_{\alpha=0}^{2D-H}\sum_{\beta=0}^{2D-H}(\alpha-\beta)2$ (9)

The average energy of distortion is

$A_E=\frac{(2R-1)}{2R},2^{-2D}\sum_{\alpha=0}^{2D-H}\sum_{\beta=0}^{2D-H}(\alpha-\beta)^2$ (10)

Here, the distortion in the selected pixels Nt is also ignored since their number is significantly less than the image size . So, the value of PSNR in the directly decrypted image is

$PSNR=10\log_{10}(A_E)$. (11)

(c) In third option, If the receiver has both the data-hiding and the encryption keys, receiver may aim to extract the embedded data and recover the original content. According to the data-hiding key, the values of D,H and R , and the $(N-N_t)R/H-N_t$ additional bits can be extracted from the encrypted image containing embedded data.

By putting the N_t LSB into their original positions, the encrypted data of the N_t selected pixels are retrieved, and their original rgb values can be correctly decrypted using the encryption keys. In the following, we will recover the original rgb values of the other pixels. Figure 6 shows the result of decrypted image after extracting the hidden data which is similar to original image.

The Table 1 gives the theoretical values of PSNR with respect to D and R.

	R=1	R=2	R=3	R=4
D=1	56.0	54.2	51.7	51.4
D=2	49.2	47.1	44.7	44.3
D=3	40.9	39.1	38.5	38.2

Denoting the decrypted pixel group index as F_g and calculate the total difference between the decrypted and estimated rgb values in the group

$D_i=\sum_{(j,k)\epsilon F(g)}[t(j,k)-q\hat{}(j,k)]$ (12)

Where the estimated rgb values is generated from the neighbours in the directly decrypted image Clearly, the estimated rgb values are only dependent on the MSB of neighbour pixels. Thus, let have 2^R different D_i corresponding to the 2^R decrypted pixel-group F_g. Among the 2^R decrypted pixel-group, there must be one that is just the original rgb values and possesses a low D_i because of the spatial correlation in natural image. To keep a low computation complexity, let R be less than ten and use only the four neighbouring pixels to calculate the estimated values.

IV. CONCLUSION

In secure transformation of data in encrypted image is to provide high network security for data transformation. Extract the hidden data and recover the original content without any error by exploiting spatial correlation in natural image if the amount of data is not too large. The proposed scheme of reversible data hiding technique is achieved through colour image instead of gray scale image to improving the capacity of hidden data. To considering gray scale image the amount of additional data is small. When using a colour image instead of gray, each bit of the red, green and blue colour components can be used, so a total of 3 bits can be stored in each pixel. It gives a relatively large amount of space to hide data. The image based data hiding technique is tried to improve the capacity of hidden data since, there is a limitation on how much information can be hidden into an image. To overcome the capacity problem, in future the video based data hiding has been achieved and to provide high security separate key should be used for encryption and decryption.

REFERENCES

[1] X. Zhang, “Separable Reversible data hiding in encrypted image,” IEEE Trans. Inform. Forensics Security, vol. 7, no. 2, pp. 826–832, Apr. 2012.

[2] W. Liu, W. Zeng, L. Dong, and Q. Yao, “Efficient compression of encrypted grayscale images,” IEEE Trans. Image Process., vol. 19, no. 4, pp. 1097–1102, Apr. 2010.

[3] X. Zhang, “Lossy compression and iterative reconstruction for encrypted image,” IEEE Trans. Inform. Forensics Security, vol. 6, no. 1, pp. 53–58, Feb. 2011.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

[4] T. Bianchi, A. Piva, and M. Barni, "Composite signal representation for fast and storage-efficient processing of encrypted signals," IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180 187, Feb. 2010.

[5] X. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255–258, Apr. 2011.

[6] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A commutative digital image watermarking and encryption method in the tree structured Haar transform domain," Signal Processing: Image Commun., vol. 26, no. 1, pp. 1–12, and 2011.

[7] W. Hong, T.-S. Chen, Y.-P. Chang, and C.-W. Shiu, "A high capacity reversible data hiding scheme using orthogonal projection and prediction error modification," Signal Process., vol. 90, pp. 2911–2922, 2010.

[8] C.-C. Chang, C.-C. Lin, and Y.-H. Chen, "Reversible data-embedding scheme using differences between original and predicted pixel values," IET Inform. Security, vol. 2, no. 2, pp. 35–46, 2008.

[9] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[10] M. Deng, T. Bianchi, A. Piva, and B. Preneel, "An efficient buyer-seller watermarking protocol based on composite signal representation," in Proc. 11th ACM Workshop Multimedia and Security, 2009, pp. 9–18.